
Notable Incident

Title	Phishing
Finding/Observation	A phishing attack occurred via email channel, where the threat actor sent phishing email containing PDF attachment with email titled as “Remittance” or something similar. The PDF contained external link which redirected the user to a fake portal where Microsoft Device Verification Code of the attacker’s device is displayed to the user. The fake portal then prompts the user to create a genuine user session on Microsoft’s site using the attacker’s Verification Code. Once, user completes the authentication, the attacker gains complete access of the user’s Microsoft account. The attacker was able to gain access of user accounts in multiple entities as the email originated from trusted/ genuine source and content of the email was relevant with the respective engagement. The lateral movement was reported by multiple entities in the securities market.
Risk Identified	- Data Exfiltration: The adversary maintained persistent access to the compromised user account, allowing for unauthorized data harvesting and exfiltration. - Lateral Movement: Utilizing the trusted identity of the compromised user, the threat actor initiated internal and external business email compromise (BEC) loops to propagate the campaign to trusted contacts.
Possible Mitigation & Recommendation	- Restrict OAuth Device Code Authentication: If not required, disable or restrict Device Code authentication. - Deploy phishing-resistant multi-factor authentication: Physical access tokens may be used. - Implement URL Filtering and Web Protection: Block access to newly registered, suspicious, or low-reputation domains. - Enforce Conditional Access Policies: Configure Conditional Access to restrict authentication from unmanaged devices, unfamiliar locations, anonymous IP addresses, and high-risk sign-in events.